A Holistic Operational Framework for Establishing Situational Awareness in Cyberspace

By Judson Dressler, William Clay Moody, Jason Koepke, and Calvert L. Bowen, III

Abstract: Our nation, including the Department of Defense, relies heavily on information systems and networking technologies to efficiently conduct a wide variety of missions across the globe. With the ever-increasing rate of cyber attacks, this dependency places the nation at risk of a loss of confidentiality, integrity, and availability of its critical information resources; degrading its ability to complete the mission. In this paper, we propose a Holistic Operational Framework for Establishing Situational Awareness in Cyberspace (HOFESAC), whose goal is to provide the nation's leadership timely and accurate information to gain an understanding of the operational cyber environment to enable strategic, operational, and tactical decision making. In doing so, we present the key information components of cyber situational awareness and present a hypothetical case study demonstrating how they must be consolidated to provide a clear and relevant picture to a commander. In addition, current organizational and technical challenges are discussed, and areas for future research are addressed.

Keywords/Key Phrases: cyber situational awareness, information security, network security

I. Introduction

Our nation's critical computer networks play a key role in our everyday lives, controlling our nation's energy, transportation, and financial systems. As such, the Department of Defense (DoD) has built operational dependency on its information systems and their associated networks. Disruption of these networks would have significantly damaging effects on our nation's ability to operate and defend itself. With the constantly increasing rate of cyber-attacks against our nation's network infrastructure and the ever-changing nature of computing, it is vitally important for the DoD to have an understanding of the cyber operating environment in order to properly secure and defend the nation.

More than a decade ago, Bass (Bass, 2000) observed that current intrusion detection technologies were not maturing at the rate of new attacks. Former Director of the National Security Agency (NSA), Mike McConnell, echoed this sentiment in February 2010 when he stated: "The United States is fighting a cyber-war today, and we are losing. It's that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking." (McConnell, 2010) Commander, United States Cyber Command (USCYBERCOM) and current Director of the NSA General Keith Alexander continued: "... to defend those networks and make good decision in exercising operational control over them ... will require much greater situational awareness and real-time visibility of intrusions into our networks." (Alexander) These concerns clearly identify the need for a comprehensive strategy to gain situational awareness over the cyber domain which enables commanders at all levels to consider cyber as they make operational decisions and direct actions for their forces.

To successfully operate in the cyberspace domain, Cyber Situational Awareness (CSA) must be effectively enabled to empower commanders and government leaders to drive action and support rapid decision-making.

In this paper we propose the Holistic Operational Framework for Establishing Situational Awareness in Cyberspace (HOFESAC). Section II provides background information and motivations for situational awareness. Section III describes related works in cyberspace research. We describe our framework in Section IV and present a case study in Section V. Challenges to establishing cyberspace situational awareness are discussed in Section VI. Sections VII and VIII present conclusions and areas for future research, respectively.

II. Background and Motivation

Defining the term "situational awareness" is almost as hard as actually building situational awareness. DoD joint doctrine does not define situational awareness in its Dictionary of Military and Associated Terms, JP 1-02, though situational awareness is used in the definition of four other terms: blue force tracking, common operational picture, United States Strategic Command's Global Network Operations Center, and national operations center. The closest definition in JP 1-02 was of "battlespace awareness", but it has been removed from the latest version.

> Battlespace Awareness —Knowledge and understanding of the operational area's environment, factors, and conditions, to include the status of friendly and adversary forces, neutrals and noncombatants, weather and terrain, that enables timely, relevant, comprehensive, and accurate

assessments, in order to successfully apply combat power, protect the force, and/or complete the mission. (Department of Defense, 2010)

Since the DoD has established cyberspace as a warfighting domain, many aspects of that definition hold true in cyberspace. With the key being to enable commanders to issue orders to forces based on timely and accurate information. The ultimate goal of situational awareness in cyberspace is to maintain strategic and tactical understanding while continuously taking action or making operation risk decisions.

Achieving CSA has proven difficult to date. However, there are a series of issues to be addressed that will allow incremental progress towards CSA capabilities that enable any organization to harness the power of near real-time information supporting decision making and proactive actions. Those issues include:

- Identification of what decisions and actions the organization may need to take with respect to cyber to assure operations can be sustained
- Identification of and access to the appropriate data that supports those decisions and actions
- Analytic tools to make sense of the presented data as it relates to operations
- Technology to consolidate and visualize data for decision makers at multiple levels within the organization

III. Related Works

Network defense, and in the military realm information dominance, have been hot topics over the last decade (Li, Ou, & Rajagopalan, 2010) (Croom, 2010) (Deutsch, 2010). Computer systems have become fully integrated into our very existence, impacting how we live our lives. Most research has been focused on defining cyberspace and developing innovative ways to defend it in the ever-changing cyber environment (Stovall, 2010) (Cumiford, 2006) (Jajodia & Noel, 2009), including discussions focused on the unique challenge that most of the network infrastructure is a commercial product outside the control and protection of any one entity (Cuviello & Kobel, 2010) (Condello, 2010) (Cumiford, 2006).

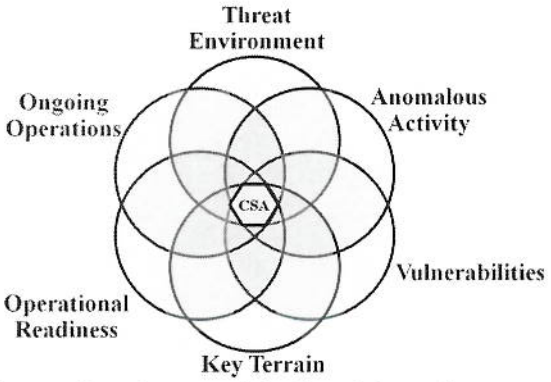
There has been considerable investment into new hardware and software technologies for intrusion detection systems (IDS), host-based security systems, and anti-virus discovery mechanisms (Bass, 2000). Comprehensive solutions for data-fusion have been presented in attempts to provide CSA (Sudit & Stoltz, 2007) (Yang, Byers, & Holsopple, 2008). Many publications in the last few years discuss security frameworks to gain insight into the situational environment (Batsell, Rao, & Shankar, 2005) (Cumiford, 2006) and even more recently, the notion of tying network security to mission assurance (Heinke, 2010) (Cumiford, 2006).

Visualization techniques using both physical and geographical layouts have been presented including multiple platforms for CSA (D'Amico & Kocka, 2005) (Gregoire & Beaudoin, 2005) (Jajodia & Noel, 2009). These studies are inherently important to CSA and the discussion of what is the optimal way to display this type of information and at what occupational level is still ongoing.

IV. Holistic Operational Framework

In the HOFESAC model, to obtain the full Cyber SA picture, there are six classes of information that need to be fused, correlated, analyzed, and visualized in near real time. The six classes are as follows:

1. Current and near-future **threat environment;**
2. Identify global threats and significant **anomalous activity**;
3. **Vulnerabilities** of our nation's computer systems and underlying infrastructure;
4. Prioritized cyber **key terrain** that allows understanding of operational and technical risks;
5. Current **operational readiness** and capability of our cyber forces and sensors; and
6. In-depth knowledge of **ongoing operations** and critical mission dependencies on our cyber assets.



As shown in Figure 1, the intersection of any combination of these classes provides more information and moves towards the sweet spot of SA. The factors from all six classes must be continuously assessed in order to provide a true, accurate and holistic representation of the domain which supports the ability to take critical actions and make decisions.

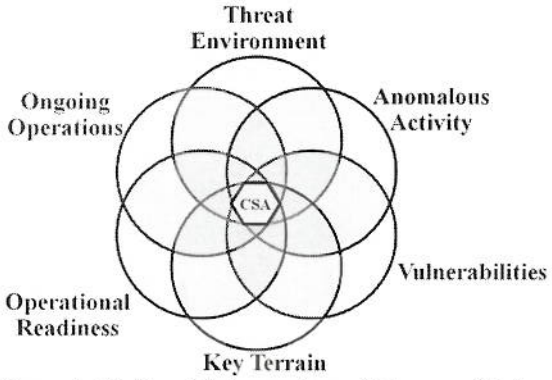


Figure 1. Notional intersection of classes of information requires continuous assessment to provide Cyber SA and enable critical actions and decisions

A. Threat Environment

To successfully defend the network, an in-depth analysis of potential threats is crucial. This includes an understanding of who would want to attack the network, what goals are they looking to achieve, and how do they normally operate. A thorough knowledge of a threat's personality and normal behaviors will assist in identifying the threat's tactics, techniques, and procedures (TTP) and developing TTPs for network defense and incident response. Assessing an attack's vector in its early stages may reveal the attacker's capability and behavioral trends, leading to projections of future intrusion activities. This awareness can reap huge rewards in the protection from and reaction to a cyber attack. It also can be used to proactively align resources to counter future attacks using similar TTPs. Development of these adversary profiles could also lead to attribution, preemptive actions, and attribution in the event of an attack.

B. Anomalous Activity

Most networks have firewalls, anti-virus, and intrusion detection systems (IDS), which operate under pre-established rules or signatures, to detect or block when an anomalous activity occurs. These tools cannot respond to a zero-day exploit or a polymorphic virus because these events do not trigger the pre-established rules. Network and host-based intrusion detection systems are essential to successfully defending the network. However, "IDS sensors can only capture systematic phenomena caused by attacks but cannot positively ascertain whether an attack has happened or succeeded" (Li, Ou, & Rajagopalan, 2010). Baseline historical and current consolidated and normalized data must be incorporated into an automated system in order to understand what is "normal" and what is "anomalous" then take actions to effectively defend against cyber threats represented by this activity.

C. Vulnerabilities

In 2010 alone, over 8,000 vulnerabilities were disclosed, a 27% increase from 2009 (Casey, 2011). Vulnerabilities are present in every system no matter how secure the system claims to be. Technology advances so rapidly that it can be virtually impossible to eradicate vulnerabilities altogether. The best one can hope for, in many cases, is

simply to minimize them. In order to assess and minimize the risk to the network, vulnerabilities of the systems and the underlying infrastructure must be known. System administrators and security specialists must have the knowledge and tools to understand the vulnerabilities of their networks and to properly test any new system or application before applying it to the network. Most importantly, these vulnerabilities must be known and continuously assessed. Leadership must be willing to allocate funds for vulnerabilities to be found and fixed.

D. Key Terrain

Though a single organization may have tens of thousands of systems ranging from desktops and mobile devices to routers and switches spread geographically across the world, not all systems have equal criticality to mission success. Defending and garnering full knowledge of all systems, accounts, and processes on the network in real time is impractical. Therefore, it is necessary to identify and prioritize key cyber assets to allow the understanding of critical risks both operationally and technically. Identification of cyber key terrain includes all critical information, systems, and infrastructure; whether owned by the organization or used in transit by its information (Pingel, 2003). That said, even these systems must be prioritized and may be less vital than a specific network link supporting a real-time airborne mission. The identification allows for prioritized defense of assets but cannot fail to consider all systems and assets in the network.

E. Operational Readiness

Organizations must know the operational readiness and capability of their cyber forces and assets. This includes the status of its tools and capabilities along with the ability of its cyber forces to protect its networks. Understanding the training status of all personnel to operate in the current threat environment and the readiness and integrity of network sensors, paths, and systems is critical. A real-time status of the network and personnel resources provides data necessary to recognize an attack and align resources which are available to appropriately respond. Mission impact is another aspect of operational readiness which is often hard to define and keep up to date. For a situational awareness picture to truly be useful, it must be operationally relevant and actionable. For this to occur, an organization must have a thorough understanding of mission dependencies based on cyber assets. With the knowledge and prioritization of intermission and mission-system dependencies, the organization can now depict to leadership the impact of a cyber event, whether an outage or attack, and the significance of securing certain assets (Heinke, 2010) (Cumiford, 2006).

F. Ongoing Operations

Lastly, information about the status of all ongoing operations (cyber and kinetic) must be fully understood by commanders at all levels. This knowledge could be used to deconflict controlled outages or upgrades to systems that are currently engaged in support of an operation. It could also be used to dynamically identify key terrain and adjust defensive TTPs during the operational window of time. Understanding which operations are being executed or soon to begin execution, allows commanders to reallocate assets as necessary to support those operations. In addition, this allows leaders to understand the operational impact of systems and their critical operational dependencies.

V. An Operational Case Study

A hypothetical operational case study is presented in order to emphasize the value of holistic fusion of data from all six classes described in our framework. In this case study, we introduce a commander and staff whom are initially presented data from the ongoing operations, key terrain, and operational readiness classes. We will show the improved situational awareness opportunities to impact the commander's decision-making process as additional information classes are considered.

A Joint Task Force (JTF) is currently conducting combat operations in an area of operations that requires the continuous flow of logistical and personnel resupply. In the operational planning process, the commander has designated his logistical support information systems as cyber key terrain. These systems operate on an unclassified military network so they can receive updates from commercial shipping and airflow systems on the Internet. The JTF commander also is aware that the network sensors deployed to protect these logistical systems are degraded due to required maintenance upgrades. The upgrades are currently scheduled for implementation by a computer network defense service provider (CND-SP) stationed in the continental United States during the next month. Lastly, the commander has an extremely proficient cyber investigative and forensics unit attending commercial certification refresher training. With this partial set of information, the commander has a good baseline of situational awareness of cyber assets and how they may impact his operations across all warfighting domains.

During the course of operations, a critical vulnerability in the outdated operating system of the logistical support system is discovered. As a DoD program of record, the potential patch for this vulnerability remains in pre-deployment testing and is not scheduled for release for another 30 days. USCYBERCOM has assessed the vulnerability and issued a high priority message across the DoD cyber enterprise announcing the details of the vulnerability. This vulnerability allows root-level access to be gained on the systems potentially enabling the deployment of malicious software on all unpatched systems. The commander is advised of the potential impact to his key logistics systems, but decides to take no action based on requirements for the continued flow of supplies and personnel supporting his operational mission set.

When the intelligence officer advises the commander on a new cyber threat report, an additional class of data (Threat Environment) is fused with the current understanding of the battlespace. In this report, it is assessed that the adversary has ever-increasing interest in disrupting and influencing the logistical flow of forces and supplies into theater. Additionally, supporting cyber assets are known to deploy Trojan-horse software on susceptible systems. This additional information of the threat environment improves the commander's understanding of the cyber environment and drives him to take decisive action to ensure his combat power will be available at the critical point in his operations. He directs his cyber force to cease with their commercial training and refocus their efforts on monitoring the behaviors of his logistical support platforms.

While reviewing the network flow and log data from the logistical system, the team discovers information included in our last class, Anomalous Activity. More than half of the logistical support systems supporting the JTF have been sending irregular sized traffic over TCP port 443 to a subnet outside of the United States. Further forensics work determines documents have been slowly exfiltrated via covert encrypted and unencrypted channels. The commander is now alarmed and initiates crisis action planning. He directs the stateside CND-SP to immediately upgrade the defensive sensors and remove the logistics systems from the network until appropriate countermeasures can be deployed to protect the systems until the patch becomes available. Further, he requests intelligence and cyber forensics support to determine which files were stolen and the potential operational impact of their loss. Now that he does not fully trust his logistics systems' information, considering future shipping schedules were the exfiltrated files, he reallocates air and naval assets to protect inbound shipping containers to protect his logistical lines of communications. Lastly, he directs his cyber forces to begin detailed log review with daily update briefings.

This case study portrays an environment where all SA information classes have an abundance of data available for consumption by an integrated system or motivated person able to fuse them together to provide the opportunity for total situational awareness. This is not today's reality. Cyber forces rarely track or concern themselves with the status of ongoing operations across all warfighting domains. Strategic and operational commanders do not know or fully understand how to determine their cyber key terrain. If they do, typically, they have not taken the required actions or time to determine and designate cyber key terrain. Additionally, the operational readiness of cyber forces is not well defined or tracked at the level needed to fully understand capabilities and how it could impact operations. In contrast, vulnerability, threat and anomalous activity data is plentiful within the intelligence and cyber communities. That said, the data is often presented to the commander in a way that information overload or technical jargon routinely make it difficult for the commander to assess the value of the information and therefore the information is discounted or ignored. Other challenges that inhibit today's ability to gain, maintain, and adjust the fusion of information that can provide SA to the commander are described in the next section.

VI. Current Challenges

Effective Cyber Situational Awareness requires that data and information be collected, analyzed, and displayed to the end customer in a timely and relevant manner. Although numerous challenges exist, the key barrier to successful implementation and execution of enterprise-wide CSA is solving the following organizational and technical challenges.

A. Organizational Fear

Gaining access to all of the necessary network data within different aspects of an organization can lead to a turf war. No entity wants to give up access to their data due to fear. Fear of humiliation in publicizing security flaws, fear of losing a competitive edge or public confidence, or fear of the proverbial 1,000 mile hammer. Regardless of the reason, this fear prevents complete situational awareness. To combat this fear, the Department of Defense must define and enforce a single information owner who can aggregate this data for analysis.

B. Data Consolidation & Normalization

Data comes in the form of technical and human collections, including IDS, network sniffers, and computer system log files. Ingesting all of the data is currently impractical but may soon become reality due to the advancement of cloud computing and the ever increasing data transfer rates. Determining the proper metrics and alert thresholds for the organization are essential for real time analysis. The data from these sources needs to be consolidated and put into a normalized format in order to be properly ingested into a CSA tool. Data refinement is simplified when a common format exists and requires a temporal calibration of the different data streams (Bass, 2000).

C. Data Synthesis

Currently, stove-piped data synthesis solutions exist across different parts of organizations that were developed separately over time without a clear coordinated cyber strategy. The challenge arises with how to fuse the data together. The fusion process requires the utilization of processing algorithms, such as Sudit's and Stotz's INFERD system, and comparison with known statistics (from USCERT, MacAfee, Norton, etc) to assess evolving situations and threats in cyberspace (Sudit & Stoltz, 2007). This data synthesis is needed for a full understanding of the normal state of the network, allowing security to move away from signature-based toward true anomaly-based detection. Intruders executing stealth TCP-based attacks on multiple geographically-separated parts of a corporate network may fall below the pre-established security thresholds. A common situational awareness tool which ideally includes all six classes of information may be able to synthesize the data and combine disparate attacks which may paint the picture of a coordinated and sophisticated enemy (Sudit & Stoltz, 2007) (Yang, Byers, & Holsopple, 2008).

D. Result Visualization and Dissemination

Until intrusion detection becomes truly machine to machine automation that responds immediately to anomalous activity, human intervention will require rapid understanding by presenting data in a visual manner. Normal situation visualization tools represent information geospatially on a map. Warfighters are used to this visual representation of disposition of forces but this depiction does not always fit well within the cyber realm. A logical picture of the network or even a temporal view may be the right answer. A dissemination plan must also be established for the actionable results. Not all information is appropriate for all personnel. Attributes that clearly identify the mission authorities and identity of the user can be used to present the appropriate data to each user.

E. Timeliness

As the amount of data, rules and signatures increase, analysis accuracy decreases and false positives increase, hampering timely detection and response. Cyber attacks occur frequently and can cause debilitating effects within milliseconds. To combat this, a finely tuned advanced threat detection engine must be used in conjunction with the known normal state to ensure the broadest possible spectrum of threats are identified and eliminate false positives as much as possible. The challenge pivots on the ability to summarize vast amounts of information at the appropriate level and then provide it to operators at the appropriate levels in a timely fashion.

VII. Conclusion

Our nation's reliance on computer networks is undeniable, and there will never be an impervious defense to all network attacks. Thus, robust situational awareness of the cyber environment, detailing what is happening, where, and what are the best available response options is absolutely critical to operations. In this paper, we developed a new approach for decision makers to assist in rapid decision making. The Holistic Operational Framework for Establishing Situational Awareness in Cyberspace integrates the six classes of information necessary (threat environment, anomalous activity, vulnerabilities, key terrain, operational readiness and ongoing operations) to effectively enable and empower commanders and government leaders to incorporate cyberspace into the decision making process. This data must be continuously analyzed to provide a true and accurate representation of the domain.

However, there still remain many challenges that must be addressed before situational awareness in cyberspace may be obtained. This paper has identified the decisions and actions the nation must take with respect to cyber, whether it be analytic tools to correlate the presented data to an operation or the technology to consolidate and visualize data for decision makers. Once addressed, the operational view of cyberspace can move from one of network assurance to a true mission assurance focused situational awareness picture.

No effective and exhaustive solution exists for recognizing the majority of cyber attacks before they occur and cause damage. With the speed of attack achievable in cyberspace, a fully developed cyber situational awareness picture is as close to an early warning system as one can achieve. Therefore, the challenges must be overcome, and situational awareness in cyberspace must be realized to enable proactive, agile, and successful network defense for the nation.

VIII. Future Work

Several key aspects of attaining situational awareness are still not well defined. Every organization depends on cyber assets to accomplish their mission. These assets can encompass thousands of computer systems, network sensors, and personnel spread across the globe. An efficient method for determining cyber key terrain to assure mission accomplishment has yet to be found.

As networks expand and data rates continue to soar, working with massive datasets in real time is becoming more common. More research is necessary in taking sensor event data, storing and efficiently correlating it to mission impact, and disseminating it in a timely manner to enable leadership to make better decisions. The advent of cloud computing may make this more achievable.

Many advances are being made in general data visualization techniques. The conventional SA tool displays network events on a geo-referenced map of the network. This method works well for battlefield awareness in ground, naval, and aerial assets, but may not be the best way to view cyberspace based on interconnections and defies geographic boundaries. Other visualization techniques need to be developed which allow SA at various levels to inform the CEO, COO, CIO, and, CISO for leadership decisions and the net defenders or system administrators for decisive actions at the operator or analyst level.

References

Alexander, K. (n.d.). Advance Questions for Lieutenant General Keith Alexander, USA Nominee for Commander, United States Cyber Command. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-srv/politics/documents/questions.pdf

Bass, T. (2000). Intrusion Detetion Systems & Multisensor Data Fusion: Creating Cyberspace Situational Awareness. *Communications of the ACM*.

Batsell, S., Rao, N., & Shankar, M. (2005). *Distributed Intrusion Detection and Attack Containment for Organizational Cyber Security.* Retrieved from Cyberspace Sciences and Information Intelligence Research Group: http://www.ioc.ornl.gov

Casey, B. (2011, March 31). *The IBM Institute for Advanced Security Expert Blog*. Retrieved from Institute for Advanced Security: http://www.instittuteforadvancedsecurity.com

Condello, K. (2010). Working Together for Real-Time Awareness. *Military Information Technology, 14*(10).

Croom, C. (2010). The Defender's "Kill Chain". *Military Information Technology, 14*(10).

Cumiford, L. (2006). Situational Awareness for Cyber Defense. *2006 CCRTS: The State of the Art and the State of the Practice.*

Cuviello, P., & Kobel, B. (2010). Cyber-Awareness is a Team Sport. *Military Information Technology, 14*(10).

D'Amico, A., & Kocka, M. (2005). *Information Assurance Visualizations for Specific Stages of Situational Awareness and Intended Uses: Lessons Learned.* Retrieved from IEEE Digital Library: http://www.ieeexplore.ieee.org

Department of Defense. (2010, August 8). *JP1-02 Dictionary of Military and Associated Terms.* Retrieved from Information for the Defense Community: www.dtic.mil/doctrine/newpubs/jp1_02.pdf

Deutsch, K. (2010). Importance of Information Dominance. *Military Information, 14*(10).

Gregoire, M., & Beaudoin, L. (2005). The Science of Mission Assurance. *Visualisation and the Common Operational Picture.*

Heinke, W. (2010). What Commanders Need to Know. *Military Information Technology, 14*(10).

Jajodia, S., & Noel, S. (2009). Topological Vulnerability Analysis. *Proceedings of the Army Research Office Cyber Situational Awareness Workshop.* Springer.

Li, J., Ou, Z., & Rajagopalan, R. (2010). Uncertainty and Risk Management in Cyber Situational Awareness. *Cyber Situational Awareness.*

McConnell, M. (2010, February 28). Mike McConnell on How to Win the Cyber-War We're Losing. *Washington Post*. Retrieved from http://www.washingtonpost.com/wp-dyn/content/article/2010/02/25/AR2010022502493.html

Pingel, T. (2003). Key Defensive Terrain in Cyberspace: A Geographic Perspective. *Proceedings of the International Conference on Politics and Information Systems (PISTA)*, (pp. 159-163). Orlando, FL.

Stovall, L. (2010). People, Processes and Technology. *Military Information Technology, 14*(10).

Sudit, M., & Stoltz, A. (2007). Information Fusion Engine for Real-time Decision-making (INFERD): A Perpetual System for Cyber Attack Tracking. *10th International Conference on Information Fusion.*

Yang, S., Byers, S., & Holsopple, J. (2008). *Intrusion Activity Projection for Cyber Situational Awareness.* Retrieved from IEEE Digital Library: http://www.ieeexplore.ieee.org